John J. Nelson (317598)
Milberg Coleman Bryson Phillips Grossman, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CHRISTINA MCCLELLAN and BILLY MOSES, individually and on behalf of all others similarly situated, Plaintiffs, v. TWITTER, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT FOR:** **1. VIOLATION OF THE FRAUDULENT, UNLAWFUL, AND UNFAIR PRONGS OF THE UCL;** **2. BREACH OF EXPRESS CONTRACT; AND** **3. UNJUST ENRICHMENT.** **DEMAND FOR JURY TRIAL**

Plaintiffs Christina McClellan and Billy Moses ("Plaintiff"), individually and on behalf of themselves and all other persons similarly situated, bring this Class Action Complaint against Twitter ("Twitter" or "Defendant"), and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

1. This action arises out of Defendant's misrepresentations and omissions to consumers regarding the purpose for which it collected and used consumers' email addresses and/or telephone numbers ("Personal Information"). At least between May 2013 and September 2019 Defendant induced consumers to provide their email addresses and telephone numbers under the false pretext of ensuring secure access to their accounts and for recovering those accounts. However, without the knowledge or consent of those who provided their email addresses and/or phone numbers, Twitter used that information for its own pecuniary gain by providing it to advertisers.

2. In a complaint filed on May 25, 2022, the U.S. Department of Justice alleged that Twitter violated the Federal Trade Commissions Act and an order issued by the U.S. FTC in 2011 (the "2011 Order") relating to deceiving users about this very conduct—namely, the extent to which Twitter maintained and protected the security and privacy of users' nonpublic contact information. Twitter has agreed to settle the complaint for $150 million.

3. The 2011 Order required that Twitter "directly or through any corporation, subsidiary, division, **website**, or other device, …, **shall not misrepresent in any manner**, expressly or by implication, the extent to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any **nonpublic consumer information.**" The 2011 Order defined "Nonpublic consumer information" as "nonpublic, individually-identifiable information from or about an individual consumer, including, but not limited to, an individual consumer's: (a) email address; (b) Internet Protocol ("IP") address **or other**

persistent identifier; …".

4. Twitter represented to its users that the Personal Information they entrusted to it would remain confidential and would only be used for security purposes. Twitter never disclosed to its users that their Personal Information was being collected for any reason other than the stated purpose of verifying user login information or allowing users to recover their accounts. All of the representations that Twitter presented to users concerning the purpose for which it demanded their email addresses and phone numbers were in the context of and concerned account security.

5. Twitter's misrepresentations and omissions regarding the purpose for which it collected email addresses and telephone numbers were material to consumers because reasonable consumers do not share this information with strangers. This is particularly so where the information will be used to target them with advertisements or solicitations or deanonymize their online identities. As a result of Twitter's deceptive practices, consumers surrendered valuable Personal Information that they expected to remain private and to be used only for security purposes. Consequently, consumers were deprived of the ability to control how this information is used and who possesses it.

JURISDICTION

1. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Moreover, this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(1) because Plaintiff McClellan is a Texas citizen and is therefore diverse from Defendant, who is a citizen of California and Delaware.

2. This Court has personal jurisdiction over Defendant because

Defendant maintains its principal place of business in this District at 1355 Market St. in San Francisco, California and has systematic and continuous contacts with the State of California and avails itself of the laws of California.

VENUE

3. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant resides within this District and because a substantial part of the events giving rise to the claims alleged herein occurred within this District. Moreover, Defendant's Terms of Service require that all disputes be heard in the state or federal courts located in San Francisco County.

PARTIES

4. Plaintiff Christina McClellan is and at all times relevant hereto was a citizen and resident of the state of Texas. Plaintiff McClellan has been a Twitter user since October 2018 and she provided her phone number to Twitter for the purpose of login verification and account recovery in or about that time.

5. When Plaintiff McClellan provided her phone number to Twitter she did so based on Twitter's admonitions to secure her account and with the understanding that Twitter would use the information exclusively for that purpose. Plaintiff read and relied on Twitter's representations concerning account security, two factor authentication ("2FA"), and account recovery and based on the information therein provided her telephone number strictly for that purpose.

6. Had Plaintiff McClellan been aware that Twitter would allow advertisers to use that information to direct advertisements at her, she either would not have provided her telephone number or would not have used Twitter's services at all.

7. To this day Plaintiff McClellan does not know which advertisers were provided access to her telephone number, how it was used, and whether it is still available for marketing purposes. Plaintiff McClellan wishes to continue to use Twitter's services in the future but she is unable to rely on Twitter's

representations concerning the use of her phone number in part because of the deceptive practices alleged herein.

8. Plaintiff Billy Moses is and at all times relevant hereto was a citizen and resident of the state of California. Plaintiff Moses has been a Twitter user since approximately 2009 and he provided his phone number and email address to Twitter for the purpose of login verification and account recovery in or about 2018.

9. When Plaintiff Moses provided his phone number to Twitter he did so based on Twitter's admonitions to secure his account and with the understanding that Twitter would use the information exclusively for that purpose. Plaintiff Moses read and relied on Twitter's representations concerning account security, 2FA, and account recovery and based on the information therein provided his telephone number and email address strictly for that purpose.

10. Had Plaintiff Moses been aware that Twitter would allow advertisers to use that information to direct advertisements at him, he either would not have provided his telephone number and email address or would not have used Twitter's services at all.

11. To this day Plaintiff Moses does not know which advertisers were provided access to his telephone number and email address, how it was used, and whether it is still available for marketing purposes. Plaintiff Moses wishes to continue to use Twitter's services in the future but he is unable to rely on Twitter's representations concerning the use of his phone number and email address in part because of the deceptive practices alleged herein.

12. Defendant Twitter, Inc. is a corporation organized and existing under the laws of the state of Delaware, with its principal place of business at 1335 Market St., San Francisco, California.

NATURE OF THE ACTION

13. Twitter operates a social media and online communication platform and is one the largest and most popular social media companies worldwide. The

platform allows registered users to broadcast short messages, known as "tweets" with which other users may interact by replying to the message or promoting it to other users by "liking" or "retweeting" the message.

14. To access the social media platform users must create a Twitter account. When Twitter users access the platform, a "timeline" is displayed to them by Twitter. The timeline presents a series of tweets from accounts the user chooses to follow, from advertisers targeting the user, or other tweets promoted or trending on the platform. The timeline also displays a search engine, recommendations for additional accounts to follow, and a list of trending topics. Twitter users also have a profile page where they can describe themselves, choose a profile picture, or view their own tweets and retweets.

15. As of September 2019, Twitter had more than 330 million monthly active users and approximately 126 million daily active users worldwide.

16. Twitter has historically failed to produce a profit for every year it reported earnings except for 2018 and 2019.[1] Twitter's annual operating costs in 2019 amounted to $3.1 billion while its revenue was slightly higher at $3.46 billion.[2]

17. Twitter provides its social media and communication platform to its hundreds of millions of users by monetizing the personally identifiable information that it collects from those users. Notably, Twitter does not charge users a monetary fee to create an account and engage with the platform. Instead, Twitter extracts value from the private information of its users that it collects and then sells to advertisers. Essentially, the cost of using Twitter to a consumer is that they must surrender exclusive control over information that they otherwise would not voluntarily provide. Put another way, in consideration for providing services,

[1] https://www.barrons.com/news/can-twitter-become-more-profitable-under-elon-musk-01650998108

[2] Twitter Q4 2019 Letter to Shareholders: https://static.seekingalpha.com/uploads/sa_presentations/382/51382/original.pdf

Twitter obtains valuable personal data from its users. That there is a cash value to the information Twitter users provide and that it can be quantified is evident from the fact that Twitter's revenue is almost exclusively derived from providing its user's information to advertisers. Indeed, Twitter evens promotes the number of "monetizable" users on its platform to advertisers as an inducement to do business with it.[3]

18. Today, Twitter derives roughly 89%, or $4.5 billion of its $5.1 billion revenue through advertising efforts. In 2019, $2.9 billion of the $3.4 billion in revenue that Twitter earned flowed from advertising. The remainder of Twitter's revenue primarily comes from licensing its data to companies which allows businesses to better understand consumer sentiment towards particular brands or anticipate trends in consumer spending or demand.[4] This data is derived from monitoring how users interact with the platform and what topics of conversation are trending. Accordingly, Twitter's economic viability depends entirely on its ability to provide consumer data and consumer attention and interactions to advertisers.

19. To use Twitter's platform, consumers agree to give up things of material value: personal data and attention. Twitter then sells for money, measurable in quantifiable units, its users' information and attention to third parties, including advertisers.

20. Twitter is attractive to advertisers not just because of the sheer number of Twitter users but because of the type and scope of information it collects about its users. The more granular and intimate the details a platform like Twitter can provide advertisers about its users, the more those advertisers are willing to use the

[3] https://business.twitter.com/en/blog/why-should-your-business-use-twitter.html#:~:text=With%20186%20million%20average%20monetizable,%2C%20and%20movement%2Dmaking%20audiences.

[4] https://www.bbc.com/news/business-24397472

platform or pay Twitter.

21. For example, Twitter can discern the interests of particular users by observing the topics of tweets they interact with or accounts that they follow. Marketers promoting products or services that cater to those interests can then direct their advertisements to those users.

22. Consumers' phone numbers and email addresses are particularly attractive to advertisers because it allows them to link the consumers' information to other databases and discern their real-world identities, e.g., where they live, what other products or services they have purchased, and other information that the consumer would ordinarily be reluctant to make available to unknown parties for advertising purposes.

23. Email addresses and phone numbers are often static and rarely change. And while a person who uses multiple social media accounts may have different user names or handles for each, phone numbers and email addresses remain the same across platforms. Because of these characteristics, phone numbers and emails can be used to identify people across platforms and to identify an individual person, much in the same way a Social Security number can be used for that purpose.

24. Telephone numbers and email addresses are also valuable to advertisers because they use the phone numbers as a data point in a process called "enhancement."[5] Once a marketer or data broker acquires a phone number it can then pair that information with other information associated with the phone number and generate individual consumer profiles. Those profiles can include details like where the consumer lives, where they shop, who they interact with, and other intimate details that the consumer would ordinarily decline to share with strangers.

25. Armed with Personal Information, advertisers can compare their own

[5] https://abcnews.go.com/Business/story?id=1402686

database of information with that which Twitter provides in order to fine tune their marketing and precisely target desirable individuals and demographics or even just to maintain consumer profiles that they can later use or sell to others. The more intimate and private details that Twitter can collect or induce its users to provide, the more revenue it derives.

26. Accordingly, Twitter is incentivized to collect specific, non-public personally identifiable information that it, in turn, can offer to advertisers to target individuals more precisely.

27. From at least May 2013, Twitter began to induce consumers to provide it with their telephone numbers and email addresses (i.e., the Personal Information) by representing to them that the information would be used solely to secure their accounts. Twitter represented to users that it required their telephone numbers and email addresses as a form of two factor authentication (2FA). Two factor authentication is a security practice that verifies the legitimacy of the first form of identification (e.g., a password or PIN) by linking it to another form of identification like a telephone number or email address specifically associated with the individual user.

28. Perversely, Twitter used the pretext of securing users' privacy to fraudulently induce them to provide non-public Personal Information that it would, in turn, offer to advertisers without the knowledge and consent of the user. Twitter misrepresented the purpose for which it collected users' phone numbers and email addresses.

29. From at least May 2013 until at least September 2019, Twitter misrepresented to users of its online communication service the extent to which it maintained and protected the security and privacy of their nonpublic contact information. While Twitter represented to users that it collected their telephone numbers and email addresses solely to secure their accounts, Twitter failed to disclose that it also used user Personal Information to aid advertisers in reaching

their preferred audiences. In exchange, Twitter handsomely profited off its users' Personal Information without their knowledge or consent.

30. Twitter's acts, omissions, and practices as alleged herein are unlawful, unfair, and deceptive and violate California Law. Plaintiffs' and Class Members have been harmed and Twitter has been unjustly enriched at their expense. Plaintiffs and Class Members seek restitution and disgorgement for Twitter's violations, as well as a permanent injunction and other equitable relief, to ensure Twitter's future compliance with the law.

SUBSTANTIVE ALLEGATIONS

Defendant's Business

31. Twitter is ostensibly a social media company but its core business model relies on monetizing its users' information by using it for advertising purposes. Twitter derives the vast majority of its revenue by collecting and aggregating the personally identifiable information of its users and selling it to advertisers who wish to reach a specific audience or demographic or bolster their understanding of the consumer marketplace.

32. In exchange for access to and use of the Twitter platform, users surrender to Twitter their personal and sensitive information as well as their time and attention. The Twitter platform by its nature is interactive and accretive. Without users interacting with the platform by posting content, commenting on the content of others, or promoting content, the platform would be of little to no interest to consumers. Conversely, the more people that use Twitter create a network effect that draws others to the platform who wish to stay informed of trends or topics or simply interact with people they know or people, like celebrities, with whom they otherwise would not have the same degrees of access.

33. The same is true of advertisers. If the Twitter platform did not have consistent and robust engagement, there would be little value to advertisers who seek to capture consumer attention and redirect it towards their own brands or

services. Accordingly, the greater number of active Twitter users, the greater value advertisers derive from their use of the platform.

34. Advertisers regularly use Twitter to promote products and services and may tweet links to websites on which users may purchase products or services.

35. Companies advertise on Twitter through a service Twitter calls "Promoted Products," which take one of three forms: (1) Promoted Tweets, which appear within a user's timeline, search results, or profile pages, similar to an ordinary tweet; (2) Promoted Accounts, which typically appear in the same format and place as other recommended accounts; and (3) Promoted Trends, which appear at the top of the list of trending topics for the day.

36. Twitter offers various services that advertisers can use to reach their existing marketing lists on Twitter, including "Tailored Audiences" and "Partner Audiences." Tailored Audiences allows advertisers to target specific groups of Twitter users by matching the telephone numbers and email addresses that Twitter collects to the advertisers' existing lists of telephone numbers and email addresses. Partner Audiences allows advertisers to import marketing lists from data brokers like Acxiom and Datalogix to match against the telephone numbers and email addresses collected by Twitter. Twitter has provided advertisers the ability to match against lists of email addresses since January 2014 and against lists of telephone numbers since September 2014. Accordingly, Twitter derives monetary value from these two types of data points.

Twitter misrepresented the purpose for which it collected and used Personal Information

37. Until at least September 17, 2019, Twitter prompted users to provide a telephone number and/or email address for the express purpose of securing or authenticating their Twitter accounts. However, unbeknownst to Twitter users, and contrary to its own Terms of Service, Twitter also used this information to serve targeted advertising and further its own business interests through its Tailored

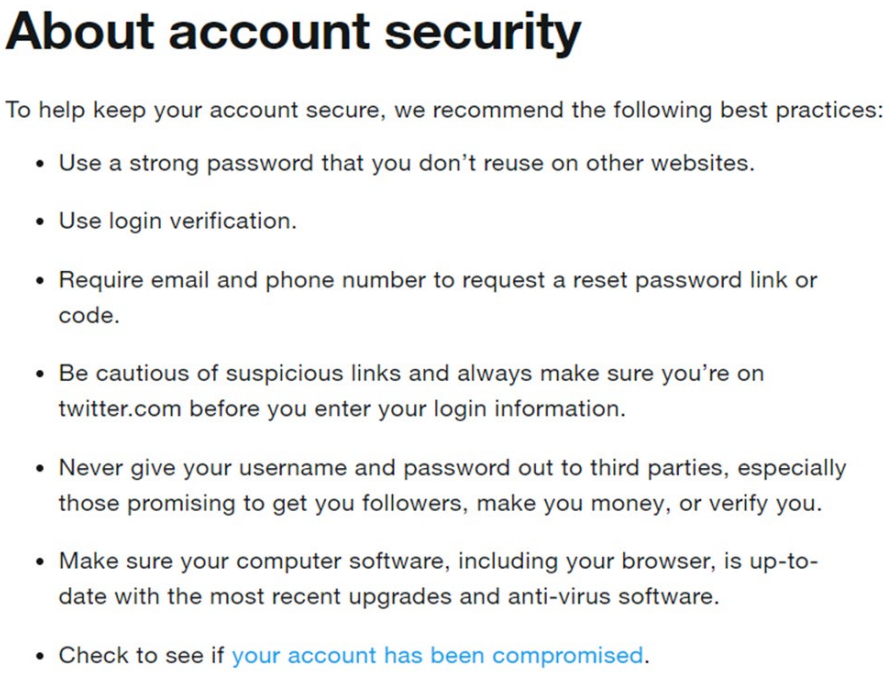
Audiences and Partner Audiences services.

38. Between at least May 2013 until at least September 2019, Twitter collected telephone numbers and email addresses from users specifically for purposes of allowing users to enable two-factor authentication, to assist with account recovery (e.g., to provide access to accounts when users have forgotten their passwords), and to re-authenticate users (e.g., to re-enable full access to an account after Twitter has detected suspicious or malicious activity). During that time, and contrary to its Terms of Service, Twitter did not disclose, or did not disclose adequately, that it used these telephone numbers and email addresses to target advertisements to those users through its Tailored Audiences and Partner Audiences services.

39. Since May 2013, Twitter has encouraged users to log into Twitter with two-factor authentication using their telephone numbers. Twitter encourages its users to use 2FA as a security practice to detect unauthorized access to user accounts. Users who enable 2FA log into their Twitter accounts with their usernames, passwords, and a code texted to their telephone numbers whenever they log in from a new or unrecognized device.

40. Twitter regularly prompts users to enable two-factor authentication through notices on their timelines and after users reset their passwords. Twitter also encourages users to turn on two-factor authentication in tweets from Twitter-operated accounts, Help Center documentation, and blog posts.

41. All of the notifications that Twitter promoted to users reference the user's need to provide their Personal Information only in the context of promoting the integrity and security of their accounts. As Twitter's Help Center instructed users on October 7, 2018:[6]



About account security

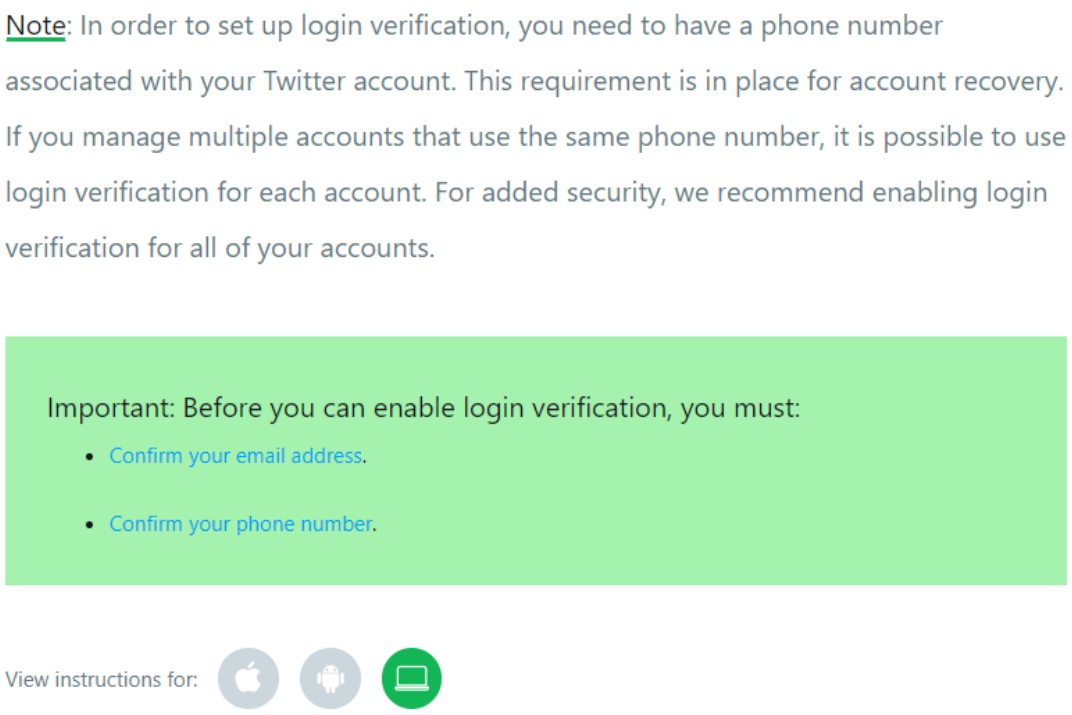
To help keep your account secure, we recommend the following best practices:

- Use a strong password that you don't reuse on other websites.
- Use login verification.
- Require email and phone number to request a reset password link or code.
- Be cautious of suspicious links and always make sure you're on twitter.com before you enter your login information.
- Never give your username and password out to third parties, especially those promising to get you followers, make you money, or verify you.
- Make sure your computer software, including your browser, is up-to-date with the most recent upgrades and anti-virus software.
- Check to see if your account has been compromised.

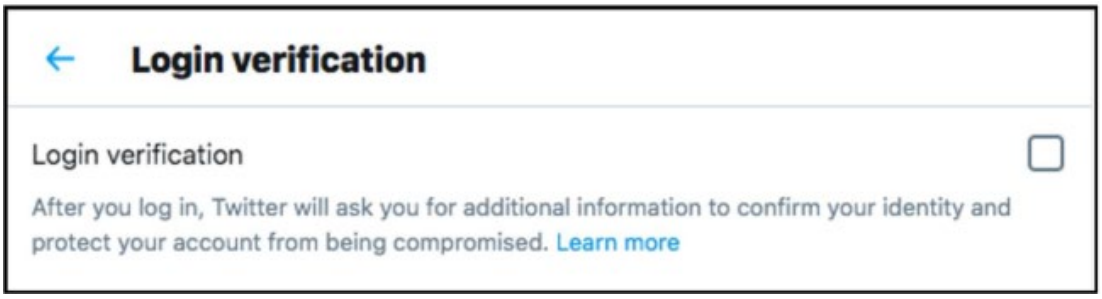
42. A post from Twitter's website as it appeared on August 31, 2019 requires that users verify their email address and phone number as a condition of using 2FA all the while stressing the importance of maintaining account security.[7] Notably, Twitter makes no mention that this information will be monetized or shared with or used by parties unknown to the user. In fact, Twitter expressly states, "[t]his requirement is in place for account recovery:"

[6] https://web.archive.org/web/20181007203622/https://help.twitter.com/en/safety-and-security/account-security-tips

[7] https://web.archive.org/web/20190830122015/https://help.twitter.com/en/managing-your-account/two-factor-authentication



43. To enable 2FA, Twitter users navigate to the "Security" tab of their account settings page where they are displayed a screen similar to the one depicted below:

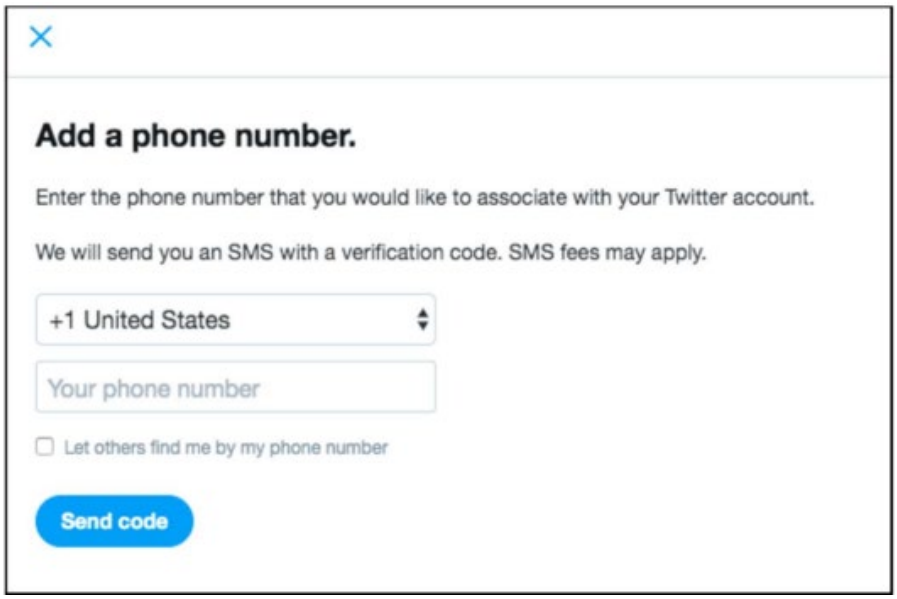


44. When users click on "Learn more," they are directed to a webpage titled, "How to use two-factor authentication." The webpage states, in relevant part:

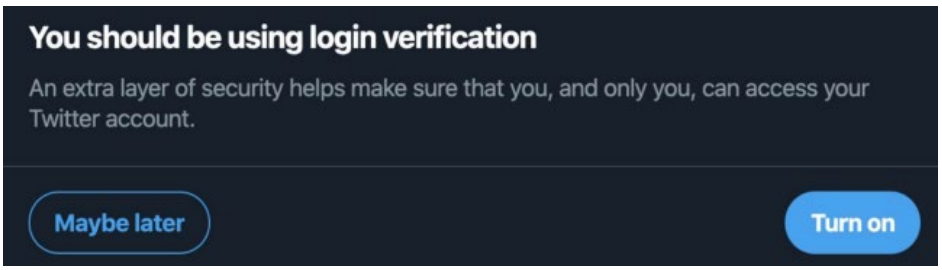
> Two-factor authentication is an extra layer of security for your Twitter account. Instead of only entering a password to log in, you'll also enter a code or use a security key. This additional step helps make sure that

you, and only you, can access your account.

45. Users who then click on "Login Verification" will be presented additional instructions about how to enable 2FA. The last screen that Twitter presents to users as they set up 2FA using a telephone number is similar to the one depicted below and, as above, makes no disclosures about using the information for advertising purposes:



46. In or about 2018, Twitter began to more aggressively induce users to enable 2FA by prompting them with posts on their timeline to ensure that they are widely viewed by Twitter users:

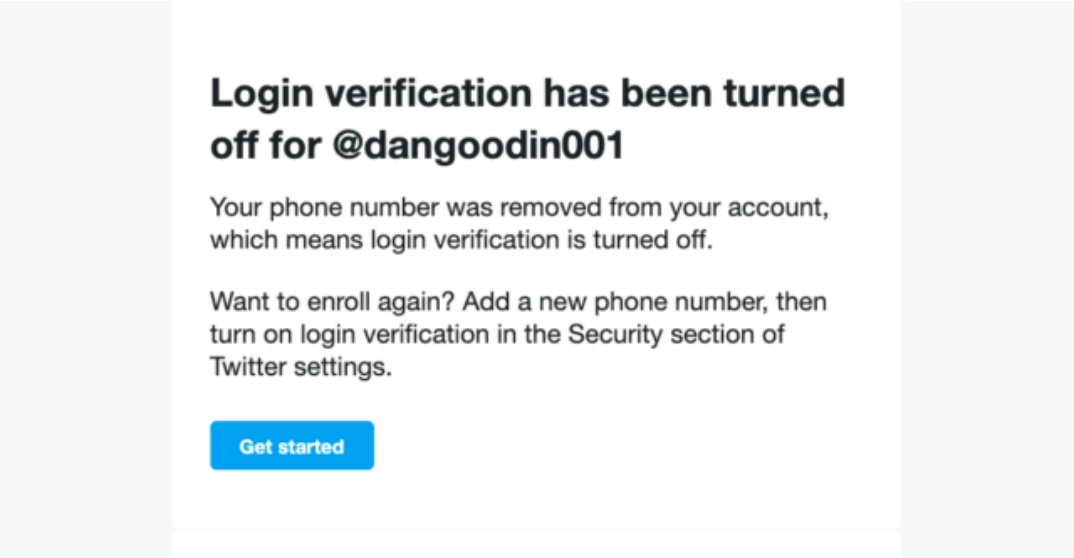


47. It was only on or about October 8, 2019, that Twitter disclosed to its

users that it had been using the information they provided for 2FA to aid advertisers in their marketing efforts while handsomely profiting in the process.

48. On information and belief, from May 2013 to September 2019, approximately two million Twitter users provided a telephone number to Twitter for the purpose of enabling 2FA. Twitter did not disclose to these users that the information would be used for any purpose aside from Twitter's stated purpose of promoting account security. Nor did Plaintiff and Class Members reasonably expect, based on Twitter's representations and Terms of Service, that Twitter would use their non-public Personal Information for any purpose unrelated to account security.

49. In fact, if a user removed their phone number, Twitter would disable the login verification feature entirely, further cementing in the user's mind that their phone numbers were being strictly used for security purposes:[8]

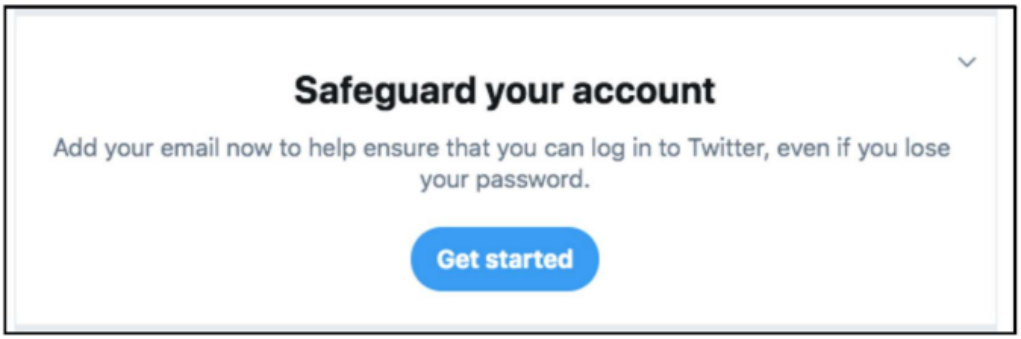


50. The fact that Twitter used the telephone numbers provided for 2FA for advertising would be material to users when deciding whether to provide a telephone number for 2FA or to continue using Twitter at all.

[8] https://arstechnica.com/information-technology/2019/10/twitter-used-phone-numbers-provided-for-2fa-to-match-users-to-advertisers/?comments=1

51. In 2015 Twitter also began encouraging users to provide their phone numbers to allow for recovery of forgotten passwords and began prompting users who had not yet provided their telephone number for 2FA to do so for password recovery purposes as reflected below:

52. In or about April of 2018, Twitter also began to prompt users to associate an email address with their account, again representing that this would allow users to recover their password in the event that they had forgotten it:



53. Through September 2019, Twitter did not disclose in any of the above prompts it directed at users or at any point in the account recovery process that it was using the telephone numbers or email addresses users provided for account recovery to target advertisements to those users.

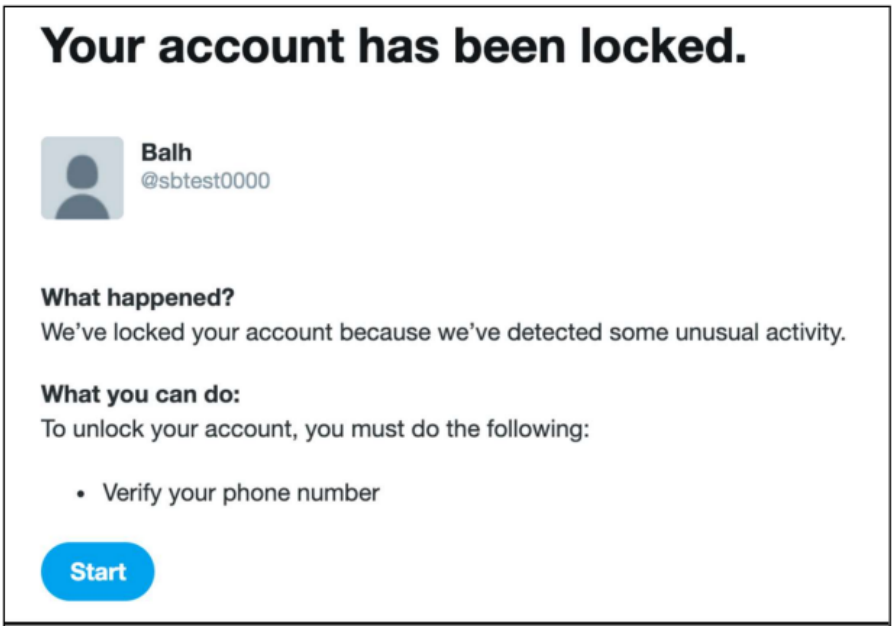
54. On information and belief, from June 2015, approximately 37 million users provided a telephone number or email address for account recovery purposes.

55. The fact that Twitter used the telephone numbers and email addresses provided by users to safeguard their accounts for advertising would be material to

users when deciding whether to provide their information for account recovery purposes or whether they wished to continue using Twitter at all.

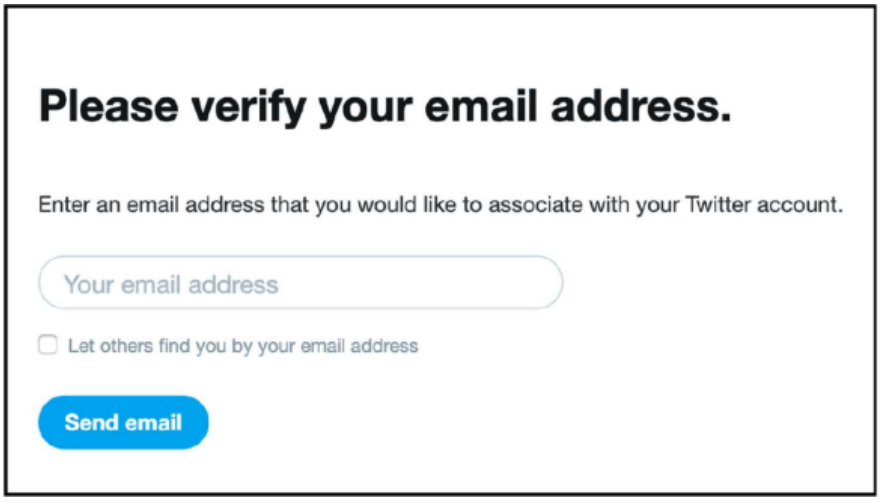
56. Twitter also required users to provide it with their telephone number or email address for account re-authentication, which would enable them to access accounts that Twitter locked due to suspicious activity it detected.

57. Twitter will block access to user accounts and demand that the user provide it with Personal Information before the account will be unlocked. When Twitter detects suspicious activity on a user's account, or suspects that the account may belong to a banned user, Twitter will prompt the user to re-authenticate the account by providing a telephone number or email address:



58. If users click "Start," they are prompted to enter a telephone number:

59. In the image below, the user is required to provide an email address to re-enable full access to their accounts, and as above, the prompt contains no mention that the information will be used for any purpose aside from verifying the user's access credentials:



60. Throughout the relevant time period, Twitter did not disclose at any point in the re-authentication process that it was using the telephone numbers or email addresses users provided for re-authentication to target advertisements to those users all the while handsomely profiting in the process. Moreover, no

reasonable user of Twitter would suspect that providing information that Twitter describes as necessary to authenticate an account would lead to that information being made available to unknown third parties.

61. On information and belief, approximately 104 million users provided a telephone number or email address in response to a prompt for re-authentication.

62. The fact that Twitter used the telephone numbers and email addresses provided for re-authentication for advertising would be material to users when deciding whether to provide their Personal Information in response to a prompt for re-authentication or to use Twitter's services at all.

Consumers guard their valuable non-public information

63. Consumers value privacy and control over their non-public personal information. In a survey of 1,000 American consumers, the average price at which they would sell their telephone number to a data broker came to $580.30 while approximately 11% said they would not sell it at all.[9]

64. To use Twitter's platform, consumers agree to give up things of material value: personal information and attention. Twitter then sells for money, measurable in quantifiable units, its users' information and attention to third parties, including advertisers. Twitter makes no secret of this and categorizes certain accounts which are active and verifiable as "monetizable" to encourage businesses to advertise on its platform to those users.[10]

65. There is an active marketplace for non-public consumer date both on the dark web[11] and for legitimate enterprises who act as data brokers like Experian or Equifax. In 2019, the data brokering industry was worth roughly $200 billion.[12]

---

[9] https://www.pcmag.com/news/would-you-sell-your-own-data-and-what-would-you-charge

[10] https://qz.com/1675900/twitter-is-finally-figuring-out-how-to-monetize-its-user-base/

[11] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[12] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[13][14] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[15] Nielsen also pay for consumers attention by paying them to monitor what programs they watch and for how long.[16]

66. While consumers understand that they may be exchanging certain of their non-public, sensitive, and/or personally identifiable information use online services, they do not agree to surrender all of their information as part of the exchange. Email, phone numbers and other non-public information is particularly guarded by consumers because that information can be used to identify them, to solicit or spam them with commercial offers, or to gather further information on them.

67. Twitter itself recognizes that its users' contact information is sensitive and that consumers have an interest in keeping it confidential. For example, in the "Privacy and Safety" section of user account settings, Twitter gives users the option to prevent others from searching for user accounts by telephone number and email, even where the other party already knows the telephone number and email address. Clearly, by providing such an option under the "Privacy and Safety" section, Twitter recognizes that consumers neither wish to share this information with the public nor have it used to discover them.[17]

68. Additionally, consumers may simply be reluctant to part with more

[13] https://datacoup.com/

[14] https://digi.me/what-is-digime/

[15] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Mar. 29, 2021).

[16] https://markets.nielsen.com/us/en/about-us/panels/ratings-and-families/

[17] https://help.twitter.com/en/safety-and-security/email-and-phone-discoverability-settings

personal information than is necessary simply because they must trust another entity to keep it safe in a time when data breaches and the theft of personally identifiable information is at an all time high. The fewer entities that possess a consumers' information the smaller the surface of the risk vector from data breaches to the consumer.

69. Once a hacker acquires a specific email address they can use it to send phishing emails, access online accounts (e.g., social media, banking), discern further personal details like names and dates of birth, or even commit identity theft.[18] Indeed, Twitter suffered a data breach from June 2021 to January 2022 in which the attacker reportedly offered for sale the emails and phone numbers of 5.4 million Twitter users for approximately $30,000.[19]

70. Similarly, an attacker who acquires a telephone number can use it to commit a "Sim Swap" where they have the victims number ported to their own device and then use that number to bypass 2FA that relies on texting or interacting with the number. The attacker can then access bank accounts, social media profiles, and other accounts to victimize a person.[20]

71. Additionally, a former Twitter employee was recently convicted of providing a foreign government with the "email addresses, phone numbers and other private data of people who had used Twitter to anonymously criticize Saudi Arabia."[21] This further underscores the sensitive nature of non-public contact information that Twitter collects and why people may wish to keep it confidential.

72. Because Twitter engaged in the deceptive conduct described above, Plaintiff and Class Members suffered substantial, cognizable, and quantifiable

---

[18] https://www.rd.com/list/what-hackers-can-do-with-email-address/

[19] https://www.ghacks.net/2022/08/08/twitter-confirms-that-a-data-breach-leaked-email-addresses-and-phone-numbers-of-users/

[20] https://www.nerdwallet.com/article/finance/sim-swap-criminals-really-number

[21] https://www.forbes.com/sites/joewalsh/2022/08/09/ex-twitter-employee-convicted-of-sending-private-data-to-saudi-government/?sh=14770382d062

economic harm.

Twitter knew that it had a duty to disclose to its users the true purpose for which it collected Personal Information.

73. At all relevant times described herein, Twitter was on notice and aware that it had a duty to adequately disclose to its users the true scope of purpose for which it collected their Personal Information.

74. In 2011, Twitter and the FTC entered into a consent order in response to Twitter's alleged violations of Section 5(a) of the FTC Act for misrepresenting the extent to which it protected consumers' privacy (the "Order").[22] Specifically, the Order prohibited Twitter using "any telephone number or email address obtained from a [u]ser before the effective date of this Order for the purpose of enabling an account security feature." While the Order did not prohibit Twitter from doing so in the future, it would first have to comply with notice, disclosure, and consent requirements of the Order.

75. The Order prohibits Twitter from misrepresenting "the extent to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, including, but not limited to, misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users."

76. Twitter violated the FTC Order, an order that is facially designed to benefit Plaintiffs and Members of the Class and to protect them from the very harm that Twitter would inflict on them. Notably, in all of the examples shown herein, Twitter makes no disclosures that would allow a reasonable consumer to understand that, in addition to providing their Personal Information for account security purposes, they were also providing it for Twitter's monetary benefit.

[22] *See* In re Twitter, Inc., C-4316, 151 F.T.C. 162 (Mar. 11, 2011) (Decision and Order)

Twitter allowed unauthorized access to and use of this information in violation of the Order and its own representations to its users. Consumers were deprived of the ability to make their own decisions regarding how their information would be used as a result of the misleading, unfair, and deceptive practices described above.

77. Irrespective of Twitter's duty to comply with the Order, Twitter represented, directly or indirectly, expressly or by implication, that it would maintain and protect the privacy of users' telephone numbers and email addresses that it collected to secure users' Twitter accounts. Twitter knew that its users' closely guarded the confidentiality of their Personal Information and that they reasonably believed and understood that Twitter would maintain its confidentiality. Nevertheless, Twitter used that information for its own pecuniary gain breaching its agreements with Plaintiffs and Class Members.

Twitter's Privacy Policy during the relevant time period

78. As a condition of using Twitter's services, users are required to agree to Twitter's Terms of Service and its Privacy Policy. The Privacy Policy in effect at the time Plaintiffs provided their Personal Information, warrants that: [23]

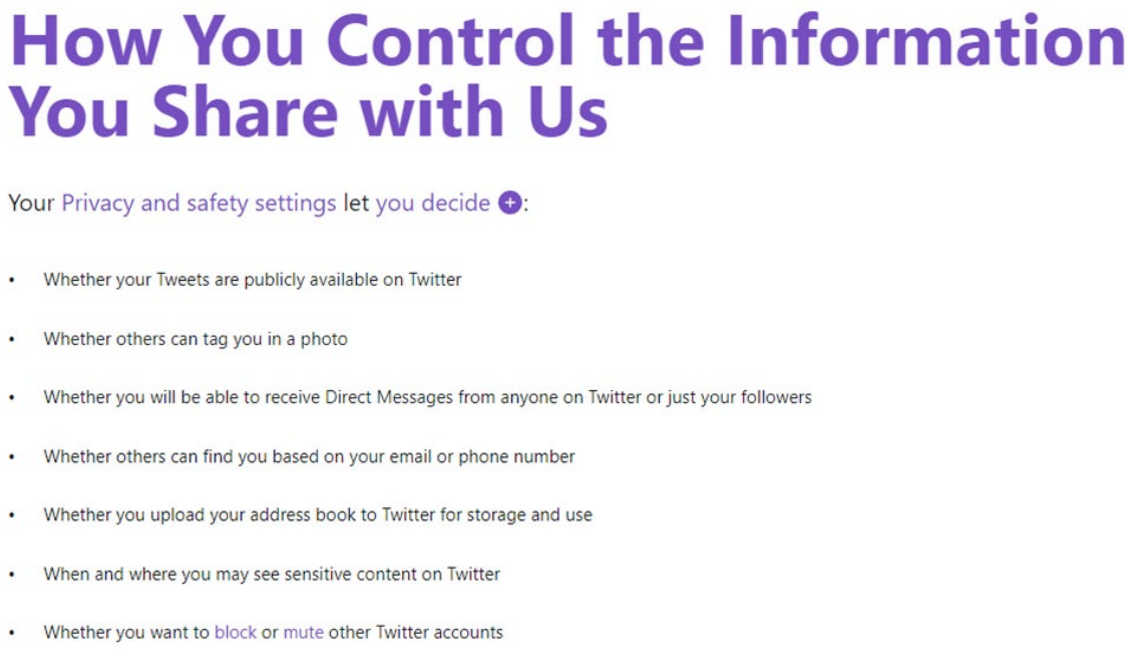
> We believe you should always know what data we collect from you and how we use it, and that you should have meaningful control over both. We want to empower you to make the best decisions about the information that you share with us.

79. Twitter violated this warranty to users by failing to adequately disclose to them, when it prompted them to input their email addresses and phone numbers for account security purposes, that Twitter would also provide that information to advertisers to more effectively target those users with ads. Twitter also misrepresented to consumers that they would have "meaningful control" over how their data is collected and used. For example, in Section 1.6 of the Privacy Policy, Twitter explains how users can control which information they share

[23] https://web.archive.org/web/20180526083315/https://twitter.com/en/privacy (Twitter's Privacy Policy as it appeared on May 26, 2018) (herein "Privacy Policy")

through the "Privacy and safety settings" section of their account:

80. Notably absent from the categories of information that Twitter represents that its users may control is the use of their Personal Information by third party advertisers:



How You Control the Information You Share with Us

Your Privacy and safety settings let you decide:

- Whether your Tweets are publicly available on Twitter
- Whether others can tag you in a photo
- Whether you will be able to receive Direct Messages from anyone on Twitter or just your followers
- Whether others can find you based on your email or phone number
- Whether you upload your address book to Twitter for storage and use
- When and where you may see sensitive content on Twitter
- Whether you want to block or mute other Twitter accounts

81. In fact, the only mention by Twitter of the use of contact information for marketing purposes is the vague statement in Section 1.3 that "Twitter also uses your contact information to market to you as your country's laws allow." This disclosure does not adequately inform users that third party advertisers and not just Twitter may use this information to advertise to the user, nor does it "empower" them to make informed decisions over how their Personal Information is used or even understand the scope of how their information will be used "as [their] country's laws allow."

82. In Section 3.1 of the Privacy Policy, Twitter represents that "you can control whether Twitter shares your personal data in this way by using the "Share your data with Twitter's business partners option in your Personalization and Data settings. in your Personalization and Data settings." Notably, the language represents to users that they could affirmatively opt-in, rather than opt-out, of

sharing their Personal Information by using the "Share your data with Twitter's business partners option." And in the same section of the Privacy Policy, Twitter further represents that

> **The information we share with these partners does not include your name, email address, phone number**, or Twitter username, but some of these partnerships allow the information we share to be linked to other personal information **if the partner gets your consent first**.

83. Twitter violated the express provisions of its Privacy Policy by misrepresenting that email addresses and phone numbers of its users would not be shared with its marketing affiliates and by expressly representing to its users that they must affirmatively consent to sharing their Personal Information before Twitter would share it with their marketing affiliates.

84. By misrepresenting the purpose for which it collected the Personal Information in security prompts and representing that "The information we share with these partners does not include your name, email address, phone number…[unless]…the partner gets your consent first" Twitter's use of users Personal Information for advertising purposes was not in conformity with Section 1.3 of the Privacy Policy and was expressly disallowed by Section 5 of FTC Act and FTC Order that required Twitter to "(a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users."

85. In addition to violating Section 5 of the FTC Act and the FTC Order, Twitter violated California law by failing to adhere to its Privacy Policy. Cal. Bus. & Prof. Code § 22576 states, in relevant part, that an "operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service" is prohibited from "knowingly and willfully [or] negligently and materially" failing to adhere to its published Privacy Policy.

STATUTE OF LIMITATIONS

86. Plaintiffs did not discover the existence of the acts complained of and alleged herein until, at the earliest, October 8, 2019 when Twitter publicly disclosed that it used its users Personal Information for advertising purposes. Nor could Plaintiffs or Class Members have discovered, through the exercise of reasonable diligence, the existence of the deceptive acts alleged herein until, at the earliest, October 8, 2019. Twitter alone possessed exclusive knowledge that it was using Personal Information entrusted to it outside the scope for which it was provided and concealed that fact from discovery until October of 2019.

CLASS ACTION ALLEGATIONS

87. Plaintiffs bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, on behalf of themselves and on behalf of all members of the following class:

> All individuals who provided their email address or telephone number to Twitter for the purpose of accessing or verifying their Twitter accounts Between May 2013 and September 17, 2019 (the "Class").

88. Excluded from the Class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

89. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

90. **Numerosity**: The Class are so numerous that joinder of all members is impracticable. Defendant collected the information of millions of its users under the

same , and the Classes are apparently identifiable within Defendants' records.

91. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant misrepresented to consumers the purpose for which it collected and used their Personal Information;

b. Whether Defendant owed a duty to the Class to disclose the purpose for which it obtained and used their Personal Information;

c. Whether Defendant breached that duty;

d. Whether Defendant was unjustly enriched at the expense of the Class.

e. Whether Defendant's conduct violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

f. Whether Defendant violated the 2011 FTC Order;

g. Whether and how Defendant utilized Personal Information with respect to third parties;

h. Whether Defendant adequately disclosed its data collection practices with respect to Personal Information;

i. Whether Defendant caused Plaintiffs' and Class Members' injuries;

j. Whether Defendant violated the unfair, unlawful, and/or fraudulent prongs of the UCL;

k. Whether Plaintiff and the other Class Members are entitled to equitable and injunctive relief;

92. **Typicality**: Plaintiffs' claims are typical of those of other Class Members because all received the same or substantially the same representations from Defendant and disclosed their Personal Information as a result.

93. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' counsel are competent and experienced in litigating privacy-related class actions.

94. **Superiority and Manageability**: Under Rule 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual Class Members are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

95. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

96. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately disclose the purpose for and its use of their Personal Information;

b. Whether Defendant breached a duty to Plaintiffs and the Class Members to keep their Personal Information confidential;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to its collection of Personal Information;

d. Whether and how Defendant used the Personal Information of Plaintiffs and Class Members with respect to third parties; and

e. Whether Class Members are entitled to restitution, disgorgement, and/or other injunctive relief as a result of Defendant's wrongful conduct.

COUNT I

Violation of California's Unfair Competition Law

Cal. Bus. & Prof. Code § 17200

(On Behalf of Plaintiffs and the Class)

97. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs.

98. By reason of the conduct alleged herein, Defendant engaged in unlawful "business practices" within the meaning of the UCL.

99. Defendant misrepresented and omitted material information regarding the purpose for which it collected and used Plaintiffs' and Class Members' email addresses and phone numbers.

100. Plaintiffs and Class Members were entitled to assume and did assume that Defendant would use the personal contact information that they provided to Twitter only for the purposes of securing and recovering their accounts.

101. Defendant did not disclose to Plaintiff and Class Members that the Personal Information that they provided in response to Twitter's representations regarding login verification and account security would be disclosed to unknown third parties or used for advertising purposes.

102. Defendant violated the unlawful prong of the UCL because Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

103. Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC §45) prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC Act prohibits acts or practices that cause or are likely to cause substantial injury to consumers, that cannot be reasonably avoided by consumers, and are not outweighed by the countervailing benefits to consumers or the marketplace. The FTC Act also prohibits material representations, omissions,

or practices that are likely to mislead reasonable consumers. This prohibition applies to all persons engaged in commerce, including Defendant.

104. Plaintiff and Class Members are consumers within the meaning of the FTC Act and Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect. The harm that occurred as alleged herein is the type of harm that the FTC Act was intended to guard against.

105. Twitter's failure to disclose or disclose adequately its reasons for collecting the Personal Information of Plaintiff and Class Members, is an unfair and deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

106. Moreover, Twitter's violation of the 2011 Order is a violation of the unlawful prong of the UCL. The Order prohibited Twitter from engaging in the exact conduct as alleged herein and was intended and implemented for the benefit of Twitter's users and the consumer marketplace. The Order specifically required that Twitter disclose the purpose for which it collected email addresses and phone number and to respect the privacy choices of its users. Twitter disregarded the Order to the detriment of Plaintiffs and the Class.

107. Additionally, Twitter violated the unlawful prong of the UCL by violating Cal. Bus. & Prof. Code § 22576, which prohibits Twitter from knowingly, negligently, and materially failing to adhere to its published Privacy Policy. Twitter's Privacy Policy represented that its users would have control over their privacy choices, must affirmatively opt-in to share that information and that email addresses and phone numbers would not be shared with third party advertisers unless "the partner gets your consent first."

108. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described misrepresentations, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

109. Plaintiffs and members of the Class read and reasonably relied on Defendant's representations concerning account security and considered those representations material in deciding whether or not to provide their Personal Information or to continue to transact with Defendant. Plaintiff and members of the Class similarly relied on Defendant to disclose any issues that contravened their express representations when deciding whether or not to transact with Defendant. Defendant misrepresented the purpose for which it collected Personal Information and omitted from disclosure the true scope of its use of Personal Information.

110. The UCL further prohibits unfair acts and practices. Defendant engaged in unfair acts and practices with respect to the collection of Personal Information by failing to fully disclose that it would also use the information for advertising purposes and its own pecuniary benefit. Twitter had within its exclusive knowledge and did not disclose to users that it had monetized their Personal Information for its own gain and at their expense. This information was not available to Plaintiffs, Class Members, or the public at large.

111. Due to Defendant's affirmative misrepresentations and material omissions the injury suffered by consumers was not reasonably avoidable through ordinary investigation. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their Personal Information was securely stored, when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

112. As a result of Defendant's material misrepresentations and omissions which were intended to and did induce Plaintiff and Class Members to surrender their Personal Information to Defendant, Plaintiff and Class Members were harmed and suffered an economic loss. Plaintiff and Class Members lost money and property as a result of Defendant's inducements in that they provided valuable, non-public and sensitive contact information and their time and attention to

Twitter. This is information and attention for which there is an active and viable marketplace, and the data has a quantifiable value. Plaintiffs have also suffered harm in the form of diminution of the value of their non-public and sensitive personally identifiable data.

113. As a result of Defendant's unlawful, unfair, and fraudulent business practices, Plaintiffs and lass Members are entitled to injunctive relief including restitution and all other remedies allowed by law.

COUNT II

BREACH OF EXPRESS CONTRACT

(On Behalf of Plaintiffs and the Class)

114. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs.

115. As a condition of using the Twitter platform, Plaintiffs and Class Members were required to and did consent to Twitter's Terms of Service, including its Privacy Policy.

116. In exchange for access, Twitter users consented to and allowed Twitter to collect and use certain of their non-public sensitive information for advertising purposes. Twitter's Privacy Policy expressly promised users that certain other information, like the Personal Information of Plaintiffs and Class Members at issue herein, would not be disclosed to third parties unless and until user's affirmatively consented to the disclosure.

117. In consideration for the use of Twitter's platform, Twitter users also provided their Personal Information and their time and attention. As described above, without users time and attention, Twitter could not monetize these users and promote its number of active users to advertisers to induce them to spend money on the Twitter platform.

118. Twitter warranted in the Privacy Policy that users would be informed as to how their data is collected and used and that users would be empowered to

make informed decisions as to what information they chose to share with Twitter. Twitter violated this provision of its contracts with users by failing to disclose in its security prompts that the email addresses and phone numbers users provided for account security would also be used for third party advertising purposes.

119. Plaintiffs and Class Members fully performed their material obligations under their contracts with Twitter. Twitter breached its contractual duties to Plaintiff and Members of the Class by failing to adequately disclose the purpose for which it collected and used their Personal Information, failing to adhere to their promise that User's must affirmatively consent to share their Personal Information with third-party advertisers, and failing to give users meaningful choice or allow them to make informed decisions as to what information they chose to share and with whom.

120. Additionally, Twitter failed to comply with its promise that Personal Information would only be used in conformity with U.S. law by violating the FTC Act and FTC Order.

121. As a direct and proximate result of Twitter's breach of contract, Plaintiffs and Class Members surrendered their time and attention and their Personal Information to Twitter and did not receive the level of service that they were promised. Twitter users were deprived of the benefit of the bargain that they struck with Twitter and the Personal information that they provided to Twitter suffered a diminution in value as a result of being shared with third parties without their consent or knowledge.

122. As a direct and proximate result of Defendants' breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Class)

123. Plaintiffs re-allege and incorporate by reference the allegations contained in the preceding paragraphs.

124. Plaintiffs allege this Count in the alternative to Count II above.

125. Throughout the relevant time period and continuing to today, Twitter's business model has entirely depended upon its collection and monetization of its users' sensitive personal information. Users agree to surrender certain of this information, in addition to their time and attention, to Twitter for the purpose of allowing them the use of its service. As part of that transaction, there is a mutual understanding that Twitter will keep certain other information entrusted to it (i.e., telephone numbers and email addresses) private, unless authorized by the user. Unbeknownst to Plaintiffs and Class Members, however, Twitter did not secure, safeguard, or protect its users Personal Information and instead offered it to be used by others for its own profit. Twitter's use of its users' Personal Information for advertising purposes was contrary to its messaging that the information was required for security purposes.

126. Plaintiffs and Class Members received services from Twitter, and Twitter was provided with, and allowed to collect and store, their Personal Information on the mutual understanding that Twitter would use that information to help them secure their accounts and not to assist advertisers in reaching them. Twitter instead willfully and intentional designed its system to provide advertisers with the very information it represented, impliedly or otherwise, that it would use only for their users' benefit.

127. Twitter designed and implemented the security features concerning login verification and 2FA and similarly designed and implemented the system on which advertisers paid for and received user data. Twitter knew or should have known that the manner in which it designed this system allowed advertisers access to information that should have been segmented and kept confidential.

128. Accordingly, Twitter knew that the manner in which they designed

their systems and maintained confidential user information violated their duties to Plaintiffs and Class Members.

129. Twitter also knew that type of information at issue herein was precisely the type of information that its users would wish to remain confidential.

130. Twitter had within its exclusive knowledge and did not disclose to users that it had monetized their Personal Information for its own gain and at their expense. This information was not available to Plaintiffs, Class Members, or the public at large.

131. Twitter also knew that was required to adhere to the FTC Order and that it must allow users to control or consent to its use of their Personal Information.

132. Plaintiffs and Class Members did not know or expect that Twitter was collecting their Personal Information and using it for advertising purposes. Had Plaintiff and Class Members known that Twitter would share the information that they provided to it with advertisers for the purpose of directing marketing efforts towards them, Plaintiff and Class Members would not have shared the information with Twitter or would not have continued to use Twitter at all.

133. By using Plaintiffs' and Class members Personal Information for its own profit and in a manner inconsistent with its representations concerning account security, Twitter put its own interests ahead of the very users who placed their trust and confidence in Twitter and benefitted it to the detriment of Plaintiffs and Class Members.

134. As a result of its conduct as alleged herein, Twitter increased its advertising revenues and increased the number of its monetizable users to allow it to derive more advertising revenue than it otherwise would have. Twitter was unjustly enriched by collecting Plaintiffs' and Class Members' Personal Information under false pretenses to the detriment of Plaintiffs and Class Members.

135. It would be inequitable, unfair, and unjust for Twitter to retain these

wrongfully obtained revenues at the expense of Plaintiffs and the Class. Twitter's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

136. Twitter's unfair and deceptive conduct to not disclose the way that it used their Personal Information caused, among other things, Plaintiffs and Class Members to surrender valuable information without remuneration.

137. As a result, Plaintiffs and Class Members paid for services that they would not have paid for had Defendant disclosed how it actually used their Personal Information.

138. Plaintiffs and each Member of the Class are entitled to restitution and non-restitutionary disgorgement in the amount by which Twitter was unjustly enriched, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all of the members of the Class, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. For an Order certifying the Class as defined herein and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse of Plaintiff's and Class Members' Personal Information;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order requiring Defendant to disclose to each Class Member whether and how their Personal Information was used, requiring Defendant to refrain from misleading and deceptive representations concerning data collection, and requiring Defendant to periodically certify their compliance with privacy standards;

D. For restitution and disgorgement of the revenues wrongfully obtained as a result of Defendant's wrongful conduct, in an amount to be determined at trial;

E. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

F. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: August 18, 2022

/s/ *John J. Nelson*
John J. Nelson (SBN 317598)
Milberg Coleman Bryson Phillips Grossman, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (917) 471-1894
Fax: (865) 522-0049
Email: jnelson@milberg.com

Gary M. Klinger*
Milberg Coleman Bryson Phillips Grossman, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
Email: gklinger@milberg.com

David K. Lietz*
Milberg Coleman Bryson Phillips Grossman, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

Counsel for Plaintiffs and the Putative Class

* *Pro Hac Vice Admission To Be Submitted*